United Nations A/C.2/58/L.19

General Assembly

Distr.: Limited
28 October 2003

Original: English

Fifty-eighth session
Second Committee
Agenda item 91 (b)
Macroeconomic policy questions: science and technology for development

Argentina, Bulgaria, Canada, Ethiopia, Romania and United States of America: draft resolution

Cybersecurity and the protection of critical information infrastructures

The General Assembly,

Noting the growing dependence of governments, businesses, other organizations and individual users on information technologies for the provision of essential goods and services, the conduct of business and the exchange of information,

Noting also the increasing dependence of the world's critical infrastructures — from production and distribution of food and water, to public health and emergency services, to energy and transportation and other vital systems — on information infrastructures that connect and increasingly control their operations,

Recognizing that this growing technological interdependence relies on a complex network of critical information infrastructure components,

Recalling its resolutions 57/239 of 20 December 2002, on the creation of a global culture of cybersecurity, 55/63 of 4 December 2000 and 56/121 of 19 December 2001, on establishing the legal basis for combating the criminal misuse of information technologies, and 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001 and 57/53 of 22 November 2002, on developments in the field of information and telecommunications in the context of international security,

Noting that, as a result of increasing interconnectivity, critical information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities that raise new security concerns,

Aware that effective critical infrastructure protection includes identifying threats to and reducing the vulnerability of critical information infrastructures,

minimizing damage and recovery time in the event of damage or attack and identifying the cause of damage or the source of attack for analysis and/or investigation,

Recognizing that effective protection requires communication, coordination, and cooperation nationally and internationally among all stakeholders, including governments, businesses and other organizations as well as individual owners and users of information technologies,

Recognizing also that gaps in access to and use of information technologies by States can diminish the effectiveness of cooperation in protecting critical information infrastructures, as well as of international cooperation in combating the criminal misuse of information technology and creating a global culture of cybersecurity, and noting the need to facilitate the transfer of information technologies, in particular to developing countries,

Noting also the work of relevant international and regional organizations in enhancing the security of critical information infrastructures,

1. *Takes note* of the value of the elements set out in the annex to the present resolution in protecting critical information infrastructures;

2. *Invites* all relevant international organizations to incorporate these elements, inter alia, for protecting critical information infrastructures in any future work on cybersecurity or critical infrastructure protection;

3. *Invites* Member States to take into account these elements, inter alia, in developing a strategy for reducing risks to critical information infrastructures;

4. *Invites* Member States and all relevant international organizations to take, inter alia, these elements and the need for critical information infrastructure protection into account in their preparations for the World Summit on the Information Society, which is to be held in Geneva from 10 to 12 December 2003 and in Tunis in 2005;

5. *Stresses* the necessity to facilitate the transfer of information technologies and capacity-building to developing countries in order to help them to protect critical information infrastructures.

Annex

Elements for protecting critical information infrastructures

1. Countries should have emergency warning networks regarding cyber-vulnerabilities, threats and incidents.

2. Countries should raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures and the role each must play in protecting them.

3. Countries should examine their infrastructures and identify interdependencies among them, thereby enhancing protection of such infrastructures.

4. Countries should promote partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information in order to prevent, investigate and respond to damage to or attacks on such infrastructures.

5. Countries should create and maintain crisis communications networks and test them to ensure that they will remain secure and stable in emergency situations.

6. Countries should ensure that data availability policies take into account the need to protect critical information infrastructures.

7. Countries should facilitate the tracing of attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other countries.

8. Countries should conduct training and exercises to enhance their response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack and should encourage stakeholders to engage in similar activities.

9. Countries should ensure that they have adequate substantive and procedural laws, such as those outlined in the Convention on Cybercrime, opened for signature by the Council of Europe on 23 November 2001, and trained personnel to enable them to investigate and prosecute attacks on critical information infrastructures and to coordinate such investigations with other countries, as appropriate.

10. Countries should engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats and incidents and coordinating investigations of attacks on such infrastructures in accordance with domestic laws.

11. Countries should promote national and international research and development and encourage the application of security technologies that are certified according to international standards.